

EXHIBIT 1

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Allegheny

County

For Prothonotary Use Only:

Docket No:

TIME STAMP

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:

- ☒ Complaint
 ☐ Writ of Summons
 ☐ Petition
 ☐ Declaration of Taking
- ☐ Transfer from Another Jurisdiction

 Lead Plaintiff's Name:
STEPHEN PFISTER

 Lead Defendant's Name:
Westinghouse Air Brake Technologies Corp. d/b/a Wabtec Corp.

 Are money damages requested? ☒ Yes ☐ No

 Dollar Amount Requested: ☐ within arbitration limits
☒ outside arbitration limits
 (check one)

 Is this a *Class Action Suit*? ☒ Yes ☐ No

 Is this an *MDJ Appeal*? ☐ Yes ☒ No

Name of Plaintiff/Appellant's Attorney: Patrick Howard

☐ Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your **PRIMARY CASE**. If you are making more than one type of claim, check the one that you consider most important.

TORT (do not include Mass Tort)

- ☐ Intentional
☐ Malicious Prosecution
☐ Motor Vehicle
☐ Nuisance
☐ Premises Liability
☐ Product Liability (does not include mass tort)
☐ Slander/Libel/ Defamation
☐ Other:

MASS TORT

- ☐ Asbestos
☐ Tobacco
☐ Toxic Tort - DES
☐ Toxic Tort - Implant
☐ Toxic Waste
☐ Other:

PROFESSIONAL LIABILITY

- ☐ Dental
☐ Legal
☐ Medical
☐ Other Professional:

CONTRACT (do not include Judgments)

- ☐ Buyer Plaintiff
☐ Debt Collection: Credit Card
☐ Debt Collection: Other
☐ Employment Dispute:
 Discrimination
☐ Employment Dispute: Other
☐ Other:

REAL PROPERTY

- ☐ Ejectment
☐ Eminent Domain/Condemnation
☐ Ground Rent
☐ Landlord/Tenant Dispute
☐ Mortgage Foreclosure: Residential
☐ Mortgage Foreclosure: Commercial
☐ Partition
☐ Quiet Title
☐ Other:

CIVIL APPEALS

- Administrative Agencies
☐ Board of Assessment
☐ Board of Elections
☐ Dept. of Transportation
☐ Statutory Appeal: Other
☐ Zoning Board
☐ Other:

MISCELLANEOUS

- ☐ Common Law/Statutory Arbitration
☐ Declaratory Judgment
☐ Mandamus
☐ Non-Domestic Relations
☐ Restraining Order
☐ Quo Warranto
☐ Replevin
☒ Other:
 DATA BREACH

SALTZ MONGELUZZI & BENDESKY P.C.

BY: PATRICK HOWARD

IDENTIFICATION NO.: 88572

1650 MARKET STREET, 52ND FLOOR

PHILADELPHIA, PA 19103

(215) 496-8282

TURKE & STRAUSS LLP

BY: RAINA BORRELLI/SAMUEL J. STRAUSS

PRO HAC VICE PENDING

613 WILLIAMSON STREET, SUITE 201

MADISON, WISCONSIN 53703

(608) 237-1775

Attorneys for Plaintiff

STEPHEN PFISTER

3302 Priscilla Dr

Erie, PA 16506

on behalf of himself and others similarly
situated,

Plaintiff,

v.

WESTINGHOUSE AIR BRAKE
TECHNOLOGIES CORPORATION, dba
WABTEC CORPORATION
1001 AirBrake Ave
Wilmerding, PA 15148

Defendant.

**ALLEGHENY COUNTY COURT
OF COMMON PLEAS**

No.

**CLASS ACTION COMPLAINT IN A
CIVIL ACTION**

JURY TRIAL DEMANDED

NOTICE

“You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by an attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.

IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

PHILADELPHIA BAR ASSOCIATION
LAWYER REFERRAL and INFORMATION
SERVICE

One Reading Center
Philadelphia, Pennsylvania 19107
(215) 238-1701”

AVISO

Se han demandado en corte. Si usted quiere defenderse contra las demandas nombradas en las páginas siguientes, tiene veinte (20) días, a partir de recibir esta demanda y la notificación para entablar personalmente o por un abogado una comparecencia escrita y también para entablar con la corte en forma escrita sus defensas y objeciones a las demandas contra usted. Sea avisado que si usted no se defiende, el caso puede continuar sin usted y la corte puede incorporar un juicio contra usted sin previo aviso para conseguir el dinero demandado en el pleito o para conseguir cualquier otra demanda o alivio solicitados por el demandante. Usted puede perder dinero o propiedad u otros derechos importantes para usted.

USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE ABOGADO (O NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO), VAYA EN PERSONA O LLAME POR TELEFONO LA OFICINA NOMBRADA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL. ESTA OFICINA PUEDE PROPORCIONARLE LA INFORMACION SOBRE CONTRATAR A UN ABOGADO.

SI USTED NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO, ESTA OFICINA PUEDE PROPORCIONARLE INFORMACION SOBRE AGENCIAS QUE OFRECEN SERVICIOS LEGALES A PERSONAS QUE CUMPLEN LOS REQUISITOS PARA UN HONORARIO REDUCIDO O NINGUN HONORARIO.

ASOCIACION DE LICENDIADOS DE FILADELFIA
SERVICO DE REFERENCA E INFORMACION
LEGAL

One Reading Center
Filadelfia, Pennsylvania 19107
Telefono: (215) 238-1701”

CLASS ACTION COMPLAINT

Plaintiff, Stephen Pfister, on behalf of himself and all others similarly situated, states as follows for his class action complaint against Defendant, Westinghouse Air Brake Technologies Corporation, dba Wabtec Corporation, (“Wabtec” or “Defendant”):

INTRODUCTION

1. On June 26, 2022, Wabtec, a digital transport and equipment solutions company headquartered in Pennsylvania, with over 37 offices throughout the United States alone, lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach by cybercriminals (“Data Breach”). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current employees.

2. On information and belief, the Data Breach began on or around March 15, 2022, when malware was introduced into Defendant’s system, and was not discovered by Wabtec until over three months later, on June 26, 2022. Following an internal investigation, Defendant learned cybercriminals gained unauthorized access to current and former employees’ personally identifiable information (“PII”) and private health information (“PHI”). PII and PHI is collectively referred to as “Sensitive Information”.

3. On information and belief, cybercriminals bypassed Defendant’s inadequate security systems to access current and former employees’ Sensitive Information in its computer systems.

4. On or around December 30, 2022 – nine months after the malware was first introduced into Defendant’s systems and over six months after the Data Breach occurred – Defendant finally began notifying victims about the breach (the “Breach Notice”) which is

attached as **Exhibit A**. However, Wabtec has not yet completed notice and continues to notify breach victims.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its current and former employees how many people were impacted, how the breach happened, or why it took the Defendant over six months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

6. Defendant's failure to timely detect and report the Data Breach made its employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

8. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former employees.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff Stephen Pfister is a former Wabtec employee and Data Breach victim. Mr. Pfister worked for Wabtec from 2018 through 2022.

11. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together

with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

12. Plaintiff, Stephen Pfister, is a natural person and citizen of Pennsylvania, residing in Erie, Pennsylvania, where he intends to remain. Mr. Pfister is a former Wabtec employee and Data Breach victim, receiving Wabtec's Breach Notice on February 22, 2023.

13. Defendant, Wabtec, is a Pennsylvania corporation with its principal place of business at 1001 AirBrake Ave Wilmerding, PA 15148-0.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under 42 Pa. Cons. Stat. § 931.

15. This Court has personal jurisdiction over Defendant because Defendant is incorporated and headquartered in Pennsylvania and conducts a significant portion of its general business in Pennsylvania.

16. Venue is proper under 231 Pa. Code § 2179 because Defendant regularly conducts business in Allegheny County.

BACKGROUND FACTS

Wabtec Corporation

17. On information and belief, Wabtec is a Pennsylvania corporation providing digital transport and equipment solutions for its customers. According to its website, Wabtec is "leading the way in safety, efficiency, reliability, innovation, and productivity."¹ Wabtec boasts a total

¹ Wabtec, <https://www.wabteccorp.com/> (last visited March 7, 2023).

revenue of \$8.36 billion² and operations in over 50 countries including the United States, Mexico, Asia, and Australia.³

18. On information and belief, Wabtec accumulates highly private Sensitive Information of its employees.

19. On information and belief, Wabtec maintains former employees' Sensitive Information for years after the employee-employer relationship is terminated.

20. In its Privacy Policy, Defendant promises that the only times Wabtec would disclose personal information would be “[with] your consent; performance of a contract with you; our legitimate interests; or compliance with our legal obligations.” Defendant further promises that they “do not sell or otherwise disclose Personal Data about you except as described [above] o at the time of collection.”⁴

21. Despite recognizing its duty to do so, on information and belief, Wabtec has not implemented reasonably cybersecurity safeguards or policies to protect employee Sensitive Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Wabtec leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employee Sensitive Information.

Wabtec Fails to Safeguard Employees' Sensitive Information

22. Plaintiff is a former employee of Wabtec.

23. As a condition of employment with Wabtec, Plaintiff provided Defendant with his Sensitive Information, including but not limited to his name, driver's license, Passport number,

² Revenue for Wabtec, Companies Market Cap, <https://companiesmarketcap.com/wabtec/revenue/> (last visited March 7, 2023).

³ Wabtec, <https://www.wabteccorp.com/> (last visited March 7, 2023).

⁴ Privacy Policy, Wabtec, <https://www.wabteccorp.com/privacy-policy#:~:text=We%20do%20not%20sell%20or,described%20in%20this%20Privacy%20Policy>. (last visited March 7, 2023).

biometric information, and Social Security number. Defendant used that Sensitive Information to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that Sensitive Information to obtain employment and payment for that employment.

24. On information and belief, Wabtec collects and maintains employees' Sensitive Information in its computer systems.

25. In collecting and maintaining the Sensitive Information, Wabtec implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

26. According to the Breach Notice, Wabtec claims to have "become aware of unusual activity on its network and promptly began an investigation" on June 26, 2022, at least six months prior to the Breach Notice. Defendant's investigation determined that "malware was introduced into certain systems as early as March 15, 2022". Additionally, Wabtec also admitted that Sensitive information was *actually stolen* during the Data Breach, confessing that "certain systems containing sensitive information [that] were subject to unauthorized access, and a certain amount of data was taken from Wabtec environment on June 26, 2022, and **was later posted** to the threat actor leak site." *See* Exh. A.

27. In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of potentially thousands of Wabtec employees' personal and highly private Sensitive Information.

28. The notorious LockBit ransomware gang claimed responsibility for the cyberattack.

⁵ LockBit is one of the most active ransomware actors, having breached over 1,000 companies

⁵ Wabtec Breach Linked to LockBit Ransomware Group, SC Media, <https://www.scmagazine.com/news/ransomware/wabtec-breach-linked-to-lockbit-ransomware-group> (last visited March 7, 2023).

worldwide⁶ and Wabtec, self-proclaimed ‘global leader’ of digital transport and equipment solutions, knew or should have known of the tactics that groups like LockBit employ.

29. With the Sensitive Information secured and stolen by LockBit, the hackers then purportedly issued a ransom demand to Wabtec. However, Wabtec has provided no public information on the ransom demand or payment.

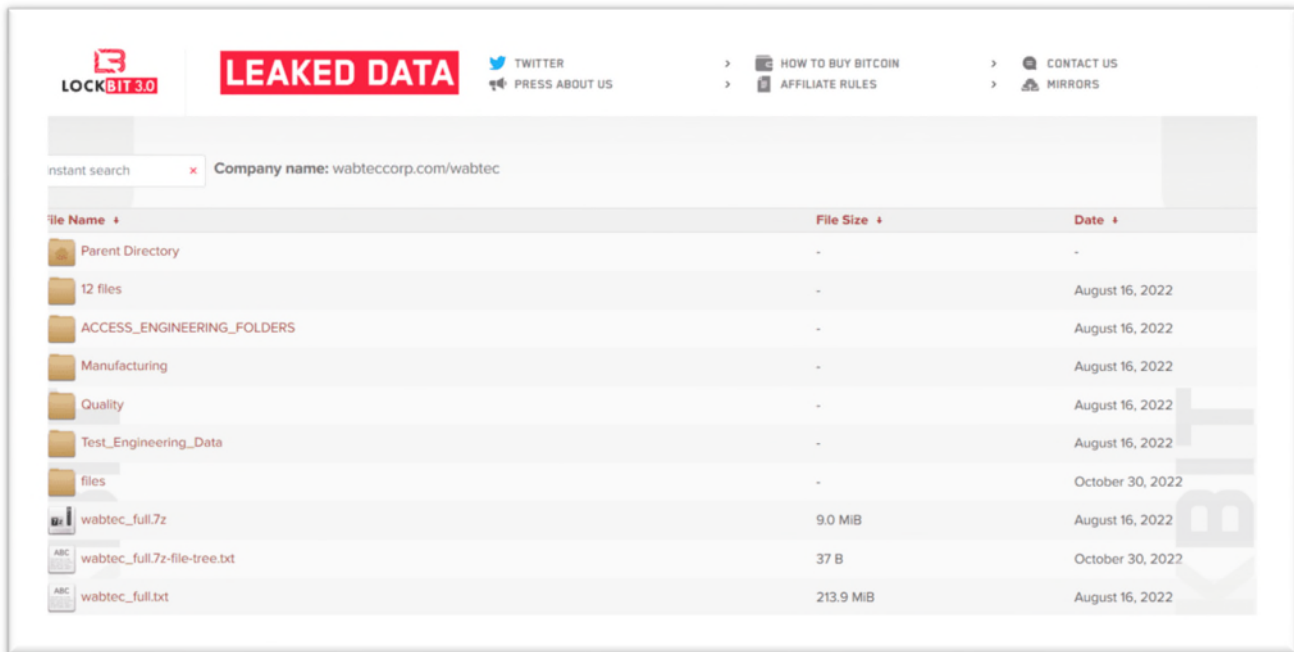
30. On August 20, 2022, the presumed deadline of LockBit’s ransom demand, LockBit released information obtained from the Breach on a data leak page.⁷



⁶ LockBit Hackers, Bloomberg, <https://www.bloomberg.com/news/articles/2023-02-02/lockbit-hackers-behind-ion-breach-also-hit-royal-mail-hospital> (last visited March 8, 2023).

⁷ Wabtec Breach, SC Media, <https://www.scmagazine.com/news/ransomware/wabtec-breach-linked-to-lockbit-ransomware-group> (last visited March 8, 2023).

31. Wabtec admitted that the following types of Sensitive Information were



The screenshot shows the LockBit 3.0 website with a search bar containing 'Company name: wabteccorp.com/wabtec'. Below the search bar is a table of leaked files.

File Name	File Size	Date
Parent Directory	-	-
12 files	-	August 16, 2022
ACCESS_ENGINEERING_FOLDERS	-	August 16, 2022
Manufacturing	-	August 16, 2022
Quality	-	August 16, 2022
Test_Engineering_Data	-	August 16, 2022
files	-	October 30, 2022
wabtec_full.7z	9.0 MiB	August 16, 2022
wabtec_full.7z-file-tree.txt	37 B	October 30, 2022
wabtec_full.txt	213.9 MiB	August 16, 2022

compromised in Defendant's Data Breach and published on LockBit's data leak page⁸ :

- a. Names;
- b. Date of Birth;
- c. Passport Number;
- d. IP Address;
- e. Employer Identification Number;
- f. Medical Record Information;
- g. Health Insurance Information;
- h. Financial Account Information;
- i. Credit and Debit Card Information;

⁸ Data Security Incident Update, Wabtec, <https://www.wabteccorp.com/data-security-incident-update-personal-data-breach-public-communication> (last visited March 8, 2023).

- j. Criminal Conviction or Offense Information;
- k. Biometric Information.

32. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff and the Class would not have accepted the Defendant's employment offer, nor provided their Sensitive Information, to Wabtec had they known that Wabtec does not take all necessary precautions to secure the personal and financial data given to it by its employees.

33. Despite its duties and alleged commitments to safeguard Sensitive Information, Wabtec does not follow industry standard practices in securing employees' Sensitive Information, as evidenced by the Data Breach and LockBit's publication of the stolen Sensitive Information.

34. In response to the Data Breach, Wabtec contends that it has or will be taking: "additional steps to reinforce the integrity and security of its systems and operations, including implementing additional procedural safeguards." Exh. A. Although Wabtec fails to expand on these alleged "additional" measures and safeguards are, such steps should have been in place *before* the Data Breach.

35. Through its Breach Notice, Wabtec also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of fraud and identity theft and fraud by reviewing your financial account statements and credit report for any anomalies." Exh. A.

36. On information and belief, Wabtec has offered a two-years of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

37. Even with two years of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

38. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

39. On information and belief, Wabtec failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

Plaintiff's Experience and Injuries

40. From approximately 2018 to 2022, Plaintiff, Stephen Pfister, was employed by Defendant.

41. As a condition to employment, Wabtec required Mr. Pfister to provide his Sensitive Information.

42. Mr. Pfister provided his Sensitive Information to Wabtec and trusted that the company would use reasonable measures to protect it according to Wabtec's internal policies and state law.

43. Wabtec deprived Mr. Pfister of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for nearly a year.

44. In fact, following the Data Breach, Plaintiff was notified through his credit monitoring system that his Sensitive Information had been published to the dark web. This demonstrates that Plaintiff's information stolen in the Data Breach has been placed in the hands of cybercriminals.

45. Plaintiff does not recall ever learning that his information was compromised in a data breach incident, other than the breach at issue in this case.

46. As a result of the Data Breach and the recommendation of Defendant's Notice, Mr. Pfister has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

47. Mr. Pfister has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Mr. Pfister fears for his personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach. Mr. Pfister has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

48. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

49. Mr. Pfister has suffered actual injury in the form of damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

50. Mr. Pfister has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

51. Mr. Pfister has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

52. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

53. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Sensitive Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

54. The types of Sensitive Information compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The employees' stolen Sensitive Information can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

55. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover,

Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

56. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

57. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their Sensitive Information is used;
- b. The diminution in value of the Sensitive Information;
- c. The compromise and continuing publication of their Sensitive Information;

- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Sensitive Information; and
- h. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in their possession.

58. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to \$1,000.00 depending on the type of information obtained.

59. The value of Plaintiff's and the proposed Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

60. It can take victims years to spot identity or PII and PHI theft, giving criminals plenty of time to use that information for cash.

61. One such example of criminals using Sensitive Information for profit is the development of “Fullz” packages.

62. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

63. The development of “Fullz” packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class’s stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

64. Defendant disclosed the Sensitive Information of Plaintiff and the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen Sensitive Information.

65. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to detect malware in its systems for over three months, demonstrates a willful and conscious disregard for privacy, and has exposed the Sensitive Information of Plaintiff and members of the proposed Class to unscrupulous operators, con-artists, and criminals.

66. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

67. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

68. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

69. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

70. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to employees’ Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

73. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients’ medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.⁹

⁹ HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

74. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.¹⁰

75. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

¹⁰ See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

- f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

76. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Offer of Credit Monitoring is Inadequate

77. At present, Wabtec has offered a mere two year long, free credit monitoring opportunity provided by Equifax to breach victims.

78. As previously alleged, Plaintiff's and the Class Members' Sensitive Information may exist on the Dark Web and in the public domain for months, or even years, before it is used for ill gains and actions. With only two years of monitoring, and no form of insurance or other protection, Plaintiff and Class Members remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

79. Therefore, the “monitoring” services offered by Wabtec are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action under Pa. R. Civ. P. 1701.

81. Plaintiff sues on behalf of himself and the proposed Class (“Class”), defined as follows:

All individuals in the United States who are current and former employees of Defendant and whose Sensitive Information was accessed without authorization in the Data Breach.

82. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

83. Plaintiff reserves the right to amend the class definition.

84. This action satisfies the numerosity, commonality, typicality, and adequacy requirements for suing as representative parties:

85. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of potentially thousands of members, far too many to join in a single action;

86. **Ascertainability**. Class members are readily identifiable from information in Defendant’s possession, custody, and control;

87. **Typicality**. Plaintiff’s claims are typical of Class member’s claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

88. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

89. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

- a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant was negligent in maintaining, protecting, and securing Sensitive Information;
- d. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's Sensitive Information;
- e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. Whether Defendant's Breach Notice was reasonable;
- g. Whether the Data Breach caused Plaintiff and the Class injuries;
- h. What the proper damages measure is; and
- i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

90. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

92. Plaintiff and members of the Class entrusted their Sensitive Information to Wabtec. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the Sensitive Information of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

93. Wabtec was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's Sensitive Information on its computer system, fully aware—as any reasonable entity of its size would be—of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

94. Defendant knew that the Sensitive Information of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the Sensitive Information of Plaintiff and the Class was wrongfully disclosed.

95. By being entrusted by Plaintiff and the Class to safeguard their Sensitive Information, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their Sensitive Information with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

96. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the Class's Sensitive Information.

97. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiff and the Class and all resulting damages.

98. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information.

99. As a result of Defendant's failure, the Sensitive Information of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Sensitive Information was disclosed to third parties without their consent.

Plaintiff and Class members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

100. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

101. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

102. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

103. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

104. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

105. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

106. Enter an award of attorneys' fees and costs, as allowed by law;

107. Enter an award of prejudgment and post-judgment interest, as provided by law;

108. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

109. Grant such other or further relief as may be appropriate under the circumstances.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

110. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

111. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

112. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's Sensitive Information.

113. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

114. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

115. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to

protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

116. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

117. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff’s and the Class’s Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

118. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

119. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant’s conduct was particularly unreasonable given the nature and amount of Sensitive Information that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

121. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

122. Had Plaintiff and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendant with their Sensitive Information.

123. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

124. Defendant's misconduct also violated Pennsylvania's data breach notification law.

125. Defendant is a business entity that maintains, stores, or manages computerized data that includes "personal information" as defined as 73 Pa. Stat. § 2302.

126. Plaintiff's and the Class's Sensitive Information includes "personal information" as defined by 73 Pa. Stat. § 2302.

127. Defendant was aware of a breach of its computer system that it believed or reasonably should have believed had caused or would cause loss or injury to residents of Pennsylvania.

128. Defendant had an obligation to disclose the Data Breach to Plaintiff and members of the Class in a timely fashion as mandated by 73 Pa. Stat. § 2303.

129. Defendant's failure to disclose the Data Breach in a timely manner as required by 73 Pa. Stat. § 2303 constitutes negligence *per se*.

130. As a direct and proximate cause of Defendant's negligence in failing to comply with 73 Pa. Stat. § 2303, Plaintiff and members of the Class sustained actual losses and damages as described herein.

131. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

132. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Wabtec fails to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

133. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

134. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

135. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

136. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

137. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

138. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

139. Enter an award of attorneys' fees and costs, as allowed by law;

140. Enter an award of prejudgment and post-judgment interest, as provided by law;

141. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

142. Grant such other or further relief as may be appropriate under the circumstances.

COUNT III
Breach of Confidence
(On Behalf of Plaintiff and the Class)

143. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

144. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of the data provided by Plaintiff and Class Members to Defendant.

145. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' Sensitive Information

would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

146. Plaintiff and Class Members provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

147. Plaintiff and Class Members also provided their respective Sensitive Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of information security practices.

148. Defendant voluntarily received in confidence Plaintiff's and Class Members' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

149. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' Sensitive Information, Plaintiff's and Class Members' Sensitive Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

150. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

151. But for Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information in violation of the parties' understanding of confidence, their Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third

parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Sensitive Information, as well as the resulting damages.

152. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Sensitive Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' Sensitive Information had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

153. As a direct and proximate result of Defendant's numerous breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

154. As a direct and proximate result of Defendant's numerous breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

155. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

156. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

157. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

158. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

159. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

160. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

161. Enter an award of attorneys' fees and costs, as allowed by law;

162. Enter an award of prejudgment and post-judgment interest, as provided by law;

163. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

164. Grant such other or further relief as may be appropriate under the circumstances.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

165. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

166. Plaintiff and the Class entrusted their Sensitive Information to Defendant at the time they entered into an employment relationship with Defendant. In so doing, Plaintiff and the Class

entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

167. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to adequately safeguard and protect their Sensitive Information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that their Sensitive Information was compromised as a result of the Data Breach.

169. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

170. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

171. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

172. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

173. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

174. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

175. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

176. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

177. Enter an award of attorneys' fees and costs, as allowed by law;

178. Enter an award of prejudgment and post-judgment interest, as provided by law;

179. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

180. Grant such other or further relief as may be appropriate under the circumstances.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

181. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

182. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

183. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Sensitive Information. They also conferred a benefit on Defendant by providing their employment services.

184. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Sensitive Information and by retaining the benefit of Plaintiff's and the Class's labor.

185. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

186. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

187. Defendant acquired the monetary benefit and Sensitive Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

188. If Plaintiff and Class Members knew that Defendant had not secured their Sensitive Information, they would not have agreed to provide their Sensitive Information to Defendant.

189. Plaintiff and Class Members have no adequate remedy at law.

190. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) the loss of the

opportunity how their Sensitive Information is used; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

191. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

192. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

193. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

194. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

195. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

196. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

197. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

198. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

199. Enter an award of attorneys' fees and costs, as allowed by law;

200. Enter an award of prejudgment and post-judgment interest, as provided by law;

201. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

202. Grant such other or further relief as may be appropriate under the circumstances.

COUNT VI
Publicity Given to Private Life
(On Behalf of Plaintiff and the Class)

203. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

204. One who gives publicity to matters concerning the private life of another, of a kind highly offensive to a reasonable man, is subject to liability to the other for invasion of his privacy.

205. As a condition of their employment, Plaintiff and the Class provided Defendant with sensitive personal information, including but not limited to: names, dates of birth, Social Security numbers, and driver's license numbers.

206. Defendant failed to employ adequate and reasonable security measures to prevent public disclosure of Plaintiff and the Class's private Sensitive Information.

207. Defendant failed to timely and reasonably notify Plaintiff and the Class about the data breach for over six months, which made Plaintiff and the Class vulnerable to identify theft.

208. As a result of the disclosure of Plaintiff's and the Class's private Sensitive Information, Plaintiff has suffered a de facto injury, which entitles them to general damages.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

209. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

210. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

211. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

212. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

213. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

214. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

215. Enter an award of attorneys' fees and costs, as allowed by law;

216. Enter an award of prejudgment and post-judgment interest, as provided by law;

217. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

218. Grant such other or further relief as may be appropriate under the circumstances.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;

- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demand that this matter be tried before a jury.

Date: March 13, 2023

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY P.C.

/s/ Patrick Howard
PATRICK HOWARD
IDENTIFICATION NO.: 88572
1650 MARKET STREET, 52ND FLOOR
PHILADELPHIA, PA 19103
(215) 496-8282
phoward@smbb.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class

VERIFICATION

The averments or denials of fact contained in the foregoing document are true based upon the signer's personal knowledge or information and belief. If the foregoing contains averments which are inconsistent in fact, signer has been unable, after reasonable investigation, to ascertain which of the inconsistent averments are true, but signer has knowledge or information sufficient to form a belief that one of them is true. This Verification is made subject to the penalties of 18 Pa. C.S. §4904, relating to falsification to authorities.



STEPHEN PFISTER

EXHIBIT A

[Home](#) >

Data Security Incident Update – Personal Data Breach Public Communication

Our Wabtec entities: Wabtec Corporation, Wabtec UK Limited and Wabtec Brasil Fabricação e Manutenção de Equipamentos Ltda., located in the US, Canada, UK and Brazil, respectively ("together Wabtec") are providing notice about an event that occurred earlier this year that affected some individuals' personal information.

What Happened. On June 26, 2022, Wabtec became aware of unusual activity on its network and promptly began an internal investigation. It was subsequently determined that malware was introduced into certain systems as early as March 15, 2022. Wabtec, with the assistance of leading cybersecurity firms, assessed the scope of the incident to, among other things, determine if personal data may have been affected. Additionally, shortly after discovery of the event, Wabtec notified the Federal Bureau of Investigation.

The forensic investigation did reveal that certain systems containing sensitive information were subject to unauthorized access, and that a certain amount of data was taken from the Wabtec environment on June 26, 2022. The information was later posted to the threat actor's leak site. On November 23, 2022, Wabtec, with the assistance of data review specialists, determined that personal information was contained within the impacted files. On December 30, 2022, Wabtec began notifying affected individuals, per relevant regulations, with a formal letter, to let them know their data was involved.

What Information Was Involved. The affected information varies by individual but includes a combination of the following data elements: First and Last Name, Date of Birth, Non-US National ID Number, Non-US Social Insurance Number or Fiscal Code, Passport Number, IP Address, Employer Identification Number (EIN), USCIS or Alien Registration Number, NHS (National Health Service) Number (UK), Medical Record/Health Insurance Information, Photograph, Gender/Gender Identity, Salary, Social Security Number (US), Financial Account Information, Payment Card Information, Account Username and Password, Biometric Information, Race/Ethnicity, Criminal Conviction or Offense, Sexual Orientation/Life, Religious Beliefs, Union Affiliation.

What Wabtec Is Doing. Wabtec is committed to and takes very seriously its responsibility to safeguard all data entrusted to it. As part of the company's ongoing commitment to the security of personal information in its care, it has taken additional steps to reinforce the integrity and security of its systems and operations, including implementing additional procedural safeguards. Wabtec has been notifying all applicable regulatory and data protection authorities, as required.

What You Can Do | Potential Consequences. While there is no indication that any specific information was or will be misused, considering the nature of the incident and of the affected personal data, we cannot rule out that there may be attempts to carry out fraudulent activity. For this reason, Wabtec encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their financial account statements and credit reports for any anomalies. Please see below for additional details in the different jurisdictions.

For More Information. If individuals have additional questions not addressed in this notice, they may contact a member of Wabtec's data privacy team by sending an email to privacy@wabtec.com. Please see below for additional contact details in the different jurisdictions.

Steps You Can Take to Help Protect Your Personal Data – US

If individuals in the US have additional questions not addressed in this notice, they may also call the dedicated assistance line at 1-888-505-4784 Monday through Friday from 9:00 am to 9:00 pm ET.

Wabtec encourages individuals to learn more about identity theft, fraud alerts, security freezes, and the steps they can take to protect themselves by contacting the consumer reporting agencies, the Federal Trade Commission, or their state Attorney General.

Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

Options Accept

Experian	TransUnion	Equifax
	Security Freeze	
Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services
	Fraud Alert	
Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information on your credit report without your expressed authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

- We encourage you to get in touch with your bank and ask about additional security measures that can be implemented by your bank to protect your bank accounts.
- Register for identity protection and credit monitoring services such as <https://www.cifas.org.uk/organisations> to guard against the risk of identity theft or fraud. If you think you have been a victim of fraud, report it to Action Fraud, the UK's national fraud and internet crime reporting centre on 0300 123 2040;
- You can consider implementing two-factor authentication (2FA) where possible to protect your online accounts from unauthorised access as described in the following publication on the National Cyber Security Centre's website: [NCSC: 2fa](#);
- Follow normal online hygiene by using secure passwords and monitoring your personal email and social media accounts for any unusual activity (for example, check your email accounts to ensure that your spam filters are set to capture any increase in unsolicited communications). Guidance concerning what to be vigilant for online can be found at: [NCSC: Data Breaches](#) and [NCSC: Password](#);
- If you receive unsolicited communications asking for personal data, do not reveal any full passwords, login details or account numbers without being certain of the identity of the person making the request. Do not click on links you do not recognise. The National Cyber Security Centre has published advice regarding suspicious emails on its website: [NCSC: Suspicious Email](#). If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) via report@phishing.gov.uk; and
- If you receive unsolicited communications from a bank or financial provider, do not transfer any money without being certain of the identity of the person making the request. The Financial Conduct Authority has published guidance on identifying financial scams on its website: [FCA: Scams](#).

Atualização sobre Incidente de Segurança de Dados – Comunicação Pública de Incidente de Segurança da Informação

Nossas entidades Wabtec: Wabtec Corporation, Wabtec UK Limited e Wabtec Brasil Fabricação e Manutenção de Equipamentos Ltda., localizadas respectivamente nos E.U.A, Canadá, Reino Unido e Brazil (em conjunto “Wabtec”) estão neste ato comunicando publicamente acerca de um evento ocorrido no início deste ano que afetou informações pessoais de alguns indivíduos.

O que aconteceu. Em 26 de junho de 2022, a Wabtec ficou ciente de uma atividade não usual nas suas redes e prontamente iniciou uma investigação interna. Foi determinado posteriormente que um malware já havia sido introduzido em alguns sistemas em 15 de março de 2022. A Wabtec, com o apoio de empresas líderes de mercado em segurança cibernética, analisou o escopo do incidente e, entre outros aspectos, determinou se dados pessoais foram afetados. Além disso, logo após a descoberta do evento, a Wabtec notificou o *Federal Bureau of Investigation* – FBI.

A investigação forense de fato revelou que certos sistemas, contendo informações sensíveis, foram acessados de modo não autorizado e que uma certa quantidade de dados foi retirada dos ambientes da Wabtec em 26 de junho de 2022. Tais informações foram posteriormente publicadas em site hacker voltado para vazamento de dados. A Wabtec, com a assistência de especialistas em revisão de dados, determinou que havia informações pessoais em alguns dos arquivos impactados. Em 30 de Dezembro de 2022, a Wabtec começou a notificar os indivíduos afetados, de acordo com as normas aplicáveis, com uma carta formal, com o objetivo de fazer com que esses indivíduos tenham conhecimento de que seus dados estavam envolvidos.

Quais Informações Estavam Envolvidas. As informações afetadas variam de acordo com o indivíduo afetado, mas incluem a combinação dos seguintes dados: Nome e Sobrenome, Data de nascimento, Número de Identificação Nacional não americano, Número de Seguridade Social ou CPF, Número de Carteira de Motorista ou de Identificação Estadual, Número de Passaporte, Registro Médico/Informações sobre Seguro de Saúde, Fotografia, Gênero/Identidade de Gênero, Salário, Número de Seguridade Social (EUA), Informações sobre Contas Financeiras, Informações sobre Cartão de Pagamento, Nome de Usuário e Senha de Contas, Informações Biométricas, Raça/Etnia, Orientação/Vida Sexual, Crenças Religiosas, Filiação a Sindicato.

O que a Wabtec Está Fazendo. A Wabtec está comprometida com e considera de forma muito séria a sua responsabilidade em proteger todos os dados confiados a nós. Como parte do compromisso permanente da empresa relacionado à segurança das informações pessoas sob o seu cuidado, ela tem implementado medidas adicionais para reforçar a integridade e a segurança dos seus sistemas e operações, incluindo a implementação de mais salvaguardas procedimentais. A Wabtec notificará todas as autoridades

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

O que Você Pode Fazer | Potenciais Consequências. Enquanto não houver indicação de que qualquer informação específica foi ou será utilizada indevidamente, considerando a natureza do incidente e dos dados pessoais afetados, não podemos afastar a possibilidade de tentativas de atividades fraudulentas. Por essa razão, encorajamos você a permanecer vigilante contra incidentes de roubo de identidade e fraude a partir da revisão dos seus extratos bancários, financeiros e informativos de créditos para identificar qualquer anomalia. Veja abaixo mais detalhes sobre o tema.

Para Mais Informações. Questões adicionais que não foram endereçadas nessa comunicação podem ser encaminhadas a um membro do time de privacidade da Wabtec por meio do e-mail privacy@wabtec.com ou o Encarregado de Dados, Henrique Tavares (henrique.tavares@wabtec.com, +55 31 999307520).

Medidas que Você Pode Tomar Para Auxiliar na Proteção dos Seus Dados Pessoais - Brasil

Seguem abaixo algumas recomendações com medidas práticas que você pode tomar no Brasil para se proteger:

- Nós encorajamos você a entrar em contato com o seu banco e solicitar medidas de segurança adicionais que podem ser implementadas pelo seu banco, a fim de proteger as suas contas bancárias;
- Se você acreditar que tenha sido vítima de fraude, faça uma denúncia à Polícia Federal: [Superintendências e delegacias](#);
- Você deve considerar implementar autenticação por dois fatores (2FA) conforme seja possível, a fim de proteger as suas contas online de acessos não autorizados, conforme descrito na seguinte publicação do Núcleo de Informação e Coordenação do Ponto BR (Nic.br): [NIC: autenticação](#);
- Siga procedimentos normais de higiene online utilizando senhas seguras e monitorando o seu e-mail pessoal e as suas contas de redes sociais contra qualquer atividade não usual (por exemplo, cheque as suas contas de e-mail para se assegurar que os filtros de spam estão configurados para capturar qualquer aumento em comunicações não solicitadas). Guia a respeito de ser vigilante online pode ser encontrado em [NIC: senhas](#) e [NIC: privacidade](#);
- Se você receber comunicações não solicitadas pedindo por dados pessoais, não revele qualquer senha, detalhes de login ou números de conta, sem ter a certeza da identidade da pessoa realizando a solicitação. Não clique em links que você não reconheça. O Núcleo de Informação e Coordenação do Ponto BR (Nic.br) publicou alguns guias a respeito de (i) redes [NIC: redes](#) (ii) computadores [NIC: computadores](#) e (iii) dispositivos móveis [NIC: dispositivos móveis](#). Se você recebeu um e-mail sobre o qual você não tem certeza da procedência, envie-o para a Política Federal conforme indicado acima;
- Se você recebeu comunicações não solicitadas de um banco ou um prestador de serviços financeiros, não transfira qualquer dinheiro sem estar certo da identidade da pessoa realizando a solicitação. O Banco Central do Brasil publicou um FAQ para identificar fraudes financeiras e como lidar com elas: [BCB: Alerta de golpes](#); e
- Você pode solicitar gratuita e livremente um reporte dos seus créditos aos gestores oficiais de banco de dados de crédito: Serasa ([Serasa](#)), ([Boa Vista](#)), SPC ([SPC](#)) e Quod ([Quod](#)).

Steps You Can Take to Help Protect Your Personal Information – Canada

If individuals in Canada have additional questions not addressed in this notice, they may also call the dedicated assistance line at 1-888-505-4784 Monday through Friday from 9:00 am to 9:00 pm ET. Additionally, individuals may contact a member of Wabtec's Data Privacy Team by emailing privacy@wabtec.com

1. Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You can access your free credit report from Equifax and TransUnion.

- Equifax:
1-800-465-7166
www.equifax.ca

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

www.transunion.ca

2. Place a Fraud Alert on Your Credit File

A fraud alert is a notice placed on your credit file that alerts creditors that you may be a victim of fraud. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the two national credit reporting agencies listed below or visiting the listed websites.

- Equifax:
1-800-465-7166
www.equifax.ca
- TransUnion:
1-800-663-9980
www.transunion.ca

3. Other Steps You Can Take

In addition to the above, we encourage you to:

- Monitor your mail for any disruption in delivery. If you notice any irregularities (such as missing financial statements, payment card statements or other documents), report such irregularities to Canada Post;
- Monitor your banking and card statements and report any suspicious activity in accounts;
- Do not reply to, click links or open attachments to messages that are suspicious. Malicious messages may contain typos or bad grammar, have formatting errors, offer unsolicited freebies or ask recipients to disclose their financial information or passwords. Always verify that the source of a message is legitimate before responding or taking action; and
- Be suspicious of any emails or text messages asking for personal information.

Nos entités Wabtec : Wabtec Corporation, Wabtec UK Limited et Wabtec Brasil Fabricação e Manutenção de Equipamentos Ltda, situées respectivement aux États-Unis, au Canada, au Royaume-Uni et au Brésil (ensemble, « Wabtec ») vous informent d'un événement survenu au début de l'année qui a affecté les informations personnelles de certaines personnes.

Que s'est-il passé. Le 26 juin 2022, Wabtec a pris conscience d'une activité inhabituelle sur son réseau et a rapidement lancé une enquête interne. Il a ensuite été déterminé qu'un logiciel malveillant avait été introduit dans certains systèmes dès le 15 mars 2022. Wabtec, avec l'aide de sociétés de cybersécurité de premier plan, a évalué la portée de l'incident pour, entre autres, déterminer si des données personnelles avaient pu être affectées. En outre, peu après la découverte de l'événement, Wabtec a informé le *Federal Bureau of Investigation*, aux États-Unis.

L'enquête judiciaire a révélé que certains systèmes contenant des informations sensibles ont fait l'objet d'un accès non autorisé et qu'un certain nombre de données ont été extraites de l'environnement de Wabtec le 26 juin 2022. Ces informations ont ensuite été publiées sur le site de fuite de l'acteur de la menace. Le 23 novembre 2022, Wabtec, avec l'aide de spécialistes de l'analyse des données, a déterminé que des informations personnelles étaient contenues dans les fichiers impactés. Le 30 Décembre 2022, Wabtec a commencé à notifier les personnes concernées, conformément aux réglementations pertinentes, par une lettre officielle, pour leur faire savoir que leurs données étaient concernées.

Quelles sont les informations concernées. Les informations concernées varient selon les individus mais comprennent une combinaison des éléments de données suivants : Nom et Prénom, Date de naissance, Numéro d'assurance sociale ou code fiscal non

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

Ce que fait Wabtec. Wabtec s'engage et prend très au sérieux sa responsabilité de protéger toutes les données qui lui sont confiées. Dans le cadre de son engagement permanent envers la sécurité des informations personnelles qui lui sont confiées, la société a pris des mesures supplémentaires pour renforcer l'intégrité et la sécurité de ses systèmes et de ses opérations, notamment en mettant en place des garanties procédurales supplémentaires. Wabtec a notifié toutes les autorités réglementaires et de protection des données applicables, tel que requis.

Ce que vous pouvez faire | Conséquences potentielles. Bien que rien n'indique que des informations spécifiques ont été ou seront utilisées à mauvais escient, compte tenu de la nature de l'incident et des données personnelles concernées, nous ne pouvons exclure la possibilité de tentatives d'activités frauduleuses. Pour cette raison, Wabtec encourage les personnes à rester vigilantes face aux incidents d'usurpation d'identité et de fraude en examinant leurs relevés de comptes financiers et leurs rapports de crédit pour détecter toute anomalie. Veuillez voir ci-dessous pour plus de détails.

Pour plus d'informations. Si les individus concernés ont des questions supplémentaires qui ne sont pas abordées dans cet avis, ils peuvent appeler la ligne d'assistance dédiée à cet effet au numéro de téléphone du centre d'appels 1-888-505-4784 du lundi au vendredi partir de 9 :00 am à 9 :00 pm ET. En outre, les personnes peuvent contacter un membre de l'équipe de confidentialité des données de Wabtec en envoyant un courriel à privacy@wabtec.com.

Mesures que vous pouvez prendre pour aider à protéger vos renseignements personnels – Canada

1. Surveillez vos comptes

Nous vous encourageons à rester vigilant face aux incidents d'usurpation d'identité et de fraude, à examiner vos relevés de compte et à surveiller vos rapports de crédit pour détecter toute activité suspecte. Vous pouvez accéder gratuitement à votre dossier de crédit auprès d'Equifax et de TransUnion.

- Equifax:
1-800-465-7166
www.equifax.ca
- TransUnion:
1-800-663-9980
www.transunion.ca

2. Placez une alerte à la fraude sur votre dossier de crédit

Une alerte à la fraude est un avis placé sur votre dossier de crédit qui avertit les créanciers que vous pourriez être victime d'une fraude. Il existe également deux types d'alertes à la fraude que vous pouvez placer sur votre dossier de crédit pour avertir vos créanciers que vous pourriez être victime d'une fraude : une alerte initiale et une alerte prolongée. Vous pouvez demander qu'une alerte initiale à la fraude soit placée sur votre dossier de crédit si vous pensez avoir été, ou être sur le point d'être, victime d'un vol d'identité. Une alerte initiale à la fraude reste sur votre dossier de crédit pendant au moins 90 jours. Une alerte prolongée peut être placée sur votre dossier de crédit si vous avez déjà été victime d'une usurpation d'identité et que vous disposez des preuves documentaires appropriées. Une alerte de fraude prolongée reste sur votre dossier de crédit pendant sept ans. Vous pouvez placer une alerte à la fraude sur votre dossier de crédit en appelant le numéro gratuit de l'une des deux agences nationales d'évaluation du crédit énumérées ci-dessous ou en consultant les sites Web indiqués

- Equifax:
1-800-465-7166
www.equifax.ca
- TransUnion:
1-800-663-9980
www.transunion.ca

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.

- Surveiller votre courrier pour déceler toute perturbation dans la livraison. Si vous remarquez des irrégularités (comme des états financiers, des relevés de cartes de paiement ou d'autres documents manquants), signalez-les à Postes Canada ;
- Surveiller vos relevés bancaires et de cartes de paiement et signaler toute activité suspecte dans vos comptes;
- Ne répondez pas aux messages suspects, ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes. Les messages malveillants peuvent contenir des fautes de frappe ou de grammaire, présenter des erreurs de formatage, offrir des cadeaux non sollicités ou demander aux destinataires de divulguer leurs informations financières ou leurs mots de passe. Vérifiez toujours que la source d'un message est légitime avant de répondre ou de prendre des mesures ; et
- Méfiez-vous des courriels ou des SMS vous demandant des informations personnelles.

Transportation solutions that move and improve the world

At Wabtec, we help our customers overcome their toughest challenges by delivering rail and industrial solutions that improve safety, efficiency and productivity.

Wabtec Corporation

30 Isabella Street
Pittsburgh, PA 15212 - USA
Phone: **412-825-1000**
Fax: **412-825-1019**

SOLUTIONS

- Locomotive
- Freight Car
- Freight Services
- Digital Intelligence
- Transit Bus
- Transit Rail
- Mining
- Adjacent Solutions

COMPANY

- About Us
- Board of Directors
- Careers
- Caring for Our Communities
- Company Overview
- Fast Facts
- Leadership Team
- Mission, Vision, Values
- Newsroom
- Sustainability
- Speak Up, Wabtec!

INFORMATION

- Contact Us
- Customer Resources
- EHS Documents
- Supplier Resources
- Wabtec University

INVESTORS

- Analysts
- Annual Report
- Financial Summary
- Green Finance Framework
- Investor Presentation
- SEC/Edgar
- Stock Quote
- Webcasts

© 2023 Wabtec Corporation. All Rights Reserved. [Terms of Use](#) [Privacy Policy](#) [Cookies](#) [Scams or Suspicious Activity](#)
[Vulnerability Disclosure](#)

We use cookies to personalize and enhance your experience on our site. Visit our [Privacy Policy](#) to learn more or manage your personal preferences in our [Cookie Consent Tool](#). By using our site, you agree to our use of cookies.